

T S6/5/1

6/5/1

DIALOG(R)File 351:Derwent WPI

(c) 2005 Thomson Derwent. All rts. reserv.

013608276

WPI Acc No: 2001-092484/200111

XRPX Acc No: N01-069981

Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not

Patent Assignee: RICOH KK (RICO)

Inventor: KANAI Y; YACHIDA M

Number of Countries: 002 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111 B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
DE 10024753	A1	159	G06F-012/14	
JP 2000339223	A	29	G06F-012/14	
JP 2001005728	A	46	G06F-012/14	
JP 2001147898	A	11	G06F-015/00	
JP 2001154577	A	12	G09C-001/00	
JP 2001209582	A	18	G06F-012/14	
JP 2001209581	A	16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. **INDEPENDENT CLAIMS** are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74

Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA

Derwent Class: P85; T01

International Patent Class (Main): G06F-012/14; G06F-015/00

International Patent Class (Additional): G06F-003/06; G06F-009/06;
G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00

File Segment: EPI; EngPI

?

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-209581

(P2001-209581A)

(43) 公開日 平成13年 8 月 3 日 (2001. 8. 3)

(51) Int.Cl.

G 0 6 F 12/14

識別記号

3 1 0

F I

G 0 6 F 12/14

テームコード* (参考)

3 1 0 Z 5 B 0 1 7

審査請求 未請求 請求項の数15 O L (全 16 頁)

(21) 出願番号 特願2000-15091 (P2000-15091)

(22) 出願日 平成12年 1 月 24 日 (2000. 1. 24)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込 1 丁目 3 番 6 号

(72) 発明者 金井 洋一

東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

(72) 発明者 谷内田 益義

東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

(74) 代理人 100104190

弁理士 酒井 昭徳

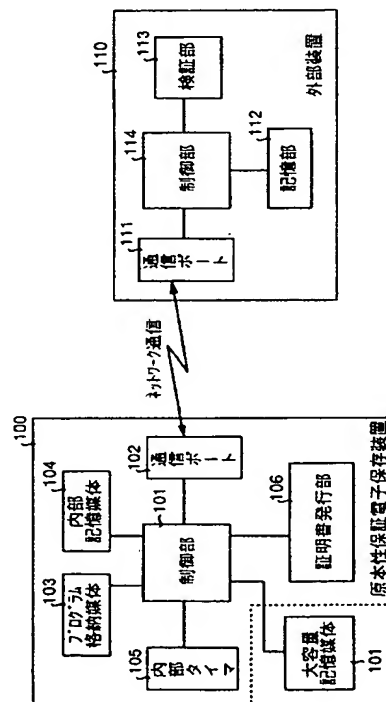
F ターム (参考) 5B017 AA06 AA08 BA05 BA07 BB02
BB10 CA09 CA16

(54) 【発明の名称】 正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証すること。

【解決手段】 原本性保証電子保存装置 106 の証明書発行部 106 が原本をコピーした複写データについての保存証明書を発行し、外部装置 110 の検証部 113 が保存証明書に基づいて複写データの正当性を検証する。



【特許請求の範囲】

【請求項 1】 所定の記憶部に記憶した原本データを複製した複製データの正当性を検証する正当性検証システムにおいて、

前記複製データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行手段と、
前記証明書発行手段により発行された証明書に基づいて、前記複製データの正当性を検証する検証手段と、
を備えたことを特徴とする正当性検証システム。

【請求項 2】 前記証明書発行手段は、
前記記憶部に記憶した前記原本データについての第 1 のハッシュ値を算定する第 1 のハッシュ値算定手段と、
前記第 1 のハッシュ値算定手段により算定された第 1 のハッシュ値を所定の秘密鍵で暗号化する暗号化手段と、
前記暗号化手段により暗号化された暗号データを証明書として出力する証明書出力手段と、
を備えたことを特徴とする請求項 1 に記載の正当性検証システム。

【請求項 3】 前記証明書発行手段は、
前記原本データについての第 1 のハッシュ値を算定する第 1 のハッシュ値算定手段と、
前記第 1 のハッシュ値算定手段により算定された第 1 のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成手段と、
前記証明内容作成手段により作成された証明内容についての第 2 のハッシュ値を算定する第 2 のハッシュ値算定手段と、
前記第 2 のハッシュ値算定手段により算定された第 2 のハッシュ値並びに前記証明内容作成手段により作成された証明内容からなる証明書を出力する証明書出力手段と、
を備えたことを特徴とする請求項 1 に記載の正当性検証システム。

【請求項 4】 前記第 1 のハッシュ値算定手段は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第 1 のハッシュ値を算定することを特徴とする請求項 3 に記載の正当性検証システム。

【請求項 5】 前記検証手段は、
前記証明書発行手段により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、
前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定手段と、
前記算定手段により算定されたハッシュ値および前記復号化手段により復号化された値を比較して、両者が一致する場合にのみ前記複製データが正当であるものと判定する判定手段と、
を備えたことを特徴とする請求項 2 に記載の正当性検証システム。

【請求項 6】 前記検証手段は、

前記証明書に含まれる前記第 2 のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、
前記証明書に含まれる証明内容についての第 3 のハッシュ値を算定する第 3 のハッシュ値算定手段と、
前記復号化手段により復号化された第 2 のハッシュ値および前記第 3 のハッシュ値算定手段により算定された第 3 のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出手段と、

10 前記読出手段により読み出された原本データについての第 4 のハッシュ値を算定する第 4 のハッシュ値算定手段と、
前記第 4 のハッシュ値算定手段により算定された第 4 のハッシュ値および前記証明内容に含まれる第 1 のハッシュ値を比較して、両者が一致する場合にのみ前記複製データが正当であるものと判定する判定手段と、
を備えたことを特徴とする請求項 3 に記載の正当性検証システム。

【請求項 7】 前記第 4 のハッシュ値算定手段は、前記読出手段により読み出された原本データの最新版の内容データとその属性情報についての第 4 のハッシュ値を算定することを特徴とする請求項 6 に記載の正当性検証システム。

【請求項 8】 所定の記憶部に記憶した原本データを複製した複製データの正当性を検証する正当性検証方法において、
前記複製データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行工程と、
前記証明書発行工程により発行された証明書に基づいて、前記複製データの正当性を検証する検証工程と、
を含んだことを特徴とする正当性検証方法。

【請求項 9】 前記証明書発行工程は、
前記記憶部に記憶した前記原本データについての第 1 のハッシュ値を算定する第 1 のハッシュ値算定工程と、
前記第 1 のハッシュ値算定工程により算定された第 1 のハッシュ値を所定の秘密鍵で暗号化する暗号化工程と、
前記暗号化工程により暗号化された暗号データを証明書として出力する証明書出力工程と、
を含んだことを特徴とする請求項 8 に記載の正当性検証方法。

【請求項 10】 前記証明書発行工程は、
前記原本データについての第 1 のハッシュ値を算定する第 1 のハッシュ値算定工程と、
前記第 1 のハッシュ値算定工程により算定された第 1 のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成工程と、
前記証明内容作成工程により作成された証明内容についての第 2 のハッシュ値を算定する第 2 のハッシュ値算定工程と、
50 前記第 2 のハッシュ値算定工程により算定された第 2 の

ハッシュ値並びに前記証明内容作成工程により作成された証明内容からなる証明書を出力する証明書出力工程と、
を含んだことを特徴とする請求項 8 に記載の正当性検証方法。

【請求項 11】 前記第 1 のハッシュ値算定工程は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第 1 のハッシュ値を算定することを特徴とする請求項 10 に記載の正当性検証方法。

【請求項 12】 前記検証工程は、
前記証明書発行工程により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、
前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定工程と、
前記算定工程により算定されたハッシュ値および前記復号化工程により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、
を含んだことを特徴とする請求項 9 に記載の正当性検証方法。

【請求項 13】 前記検証工程は、
前記証明書に含まれる前記第 2 のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、
前記証明書に含まれる証明内容についての第 3 のハッシュ値を算定する第 3 のハッシュ値算定工程と、
前記復号化工程により復号化された第 2 のハッシュ値および前記第 3 のハッシュ値算定工程により算定された第 3 のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出工程と、
前記読出工程により読み出された原本データについての第 4 のハッシュ値を算定する第 4 のハッシュ値算定工程と、
前記第 4 のハッシュ値算定工程により算定された第 4 のハッシュ値および前記証明内容に含まれる第 1 のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、
を含んだことを特徴とする請求項 10 に記載の正当性検証方法。

【請求項 14】 前記第 4 のハッシュ値算定工程は、前記読出工程により読み出された原本データの最新版の内容データとその属性情報についての第 4 のハッシュ値を算定することを特徴とする請求項 13 に記載の正当性検証方法。

【請求項 15】 前記請求項 8～14 のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証システム、正当性検証方法および記録媒体に関する。

【0002】

【従来の技術】 近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【0003】 たとえば、「金井他：原本性保証電子保存システムの開発—システムの構築—, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発, (特) 情報処理振興事業協会発行 創造的ソフトウェア育成事業およびエレクトロニック・コマース推進事業 最終成果発表会論文集 創造的ソフトウェア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【0004】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【0005】

【発明が解決しようとする課題】 しかしながら、これらの従来技術は、あくまでも原本性保証電子保存装置内部で管理されている保存データの原本性を保証するものでしかないため、そのコピーを作成して外部の装置上に保持する際に、このコピーが原本の保存データと本当に一致するか否かを効率良く保証することができないという問題がある。

【0006】すなわち、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合には、このコピーとともに原本の保存データについても当該装置上に移動しなければ、該コピーと原本の保存データが一致するか否かを調べることはできないこととなる。

【0007】ここで、本来原本としての保存データは、原本性保証電子保存装置上にのみ保持すべきであり、様々な装置上を移動させることとしたのでは、原本の保存データの喪失や原本の保存データの改ざんを招く機会を与えることとなるので、妥当ではない。なお、原本を移動する代わりに原本のコピーを移動することも考えられるが、原本の保存データをコピーしたものはすでに原本

とは言えない。

【0008】これらのことから、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することをいかに効率良く検証するかが極めて重要な課題となっている。

【0009】この発明は、上記問題（課題）に鑑みてなされたものであり、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる原本性保証電子保存システム、正当性保証方法および記録媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、請求項1に記載の発明にかかる正当性検証システムは、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証システムにおいて、前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行手段と、前記証明書発行手段により発行された証明書に基づいて、前記複写データの正当性を検証する検証手段と、を備えたことを特徴とする。

【0011】この請求項1に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【0012】また、請求項2に記載の発明にかかる正当性検証システムは、請求項1に記載の発明において、前記証明書発行手段は、前記記憶部に記憶した前記原本データについての第1のハッシュ値を算定する第1のハッシュ値算定手段と、前記第1のハッシュ値算定手段により算定された第1のハッシュ値を所定の秘密鍵で暗号化する暗号化手段と、前記暗号化手段により暗号化された暗号データを証明書として出力する証明書出力手段と、を備えたことを特徴とする。

【0013】この請求項2に記載の発明によれば、記憶部に記憶した原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる。

【0014】また、請求項3に記載の発明にかかる正当性検証システムは、請求項1に記載の発明において、前記証明書発行手段は、前記原本データについての第1のハッシュ値を算定する第1のハッシュ値算定手段と、前記第1のハッシュ値算定手段により算定された第1のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成手段と、前記証明

内容作成手段により作成された証明内容についての第2のハッシュ値を算定する第2のハッシュ値算定手段と、前記第2のハッシュ値算定手段により算定された第2のハッシュ値並びに前記証明内容作成手段により作成された証明内容からなる証明書を出力する証明書出力手段と、を備えたことを特徴とする。

【0015】この請求項3に記載の発明によれば、原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第2のハッシュ値を算定し、算定した第2のハッシュ値並びに証明内容からなる証明書を出力することとしたので、2重にハッシュ化した高い正当性を保証することができる証明書を発行することができる。

【0016】また、請求項4に記載の発明にかかる正当性検証システムは、請求項3に記載の発明において、前記第1のハッシュ値算定手段は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することを特徴とする。

【0017】この請求項4に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる。

【0018】また、請求項5に記載の発明にかかる正当性検証システムは、請求項2に記載の発明において、前記検証手段は、前記証明書発行手段により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定手段と、前記算定手段により算定されたハッシュ値および前記復号化手段により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、を備えたことを特徴とする。

【0019】この請求項5に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる。

【0020】また、請求項6に記載の発明にかかる正当性検証システムは、請求項3に記載の発明において、前記検証手段は、前記証明書に含まれる前記第2のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、前記証明書に含まれる証明内容についての第3のハッシュ値を算定する第3のハッシュ値算定手段と、前記復号化手段により復号化された第2のハッシュ値お

よび前記第3のハッシュ値算定手段により算定された第3のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出手段と、前記読出手段により読み出された原本データについての第4のハッシュ値を算定する第4のハッシュ値算定手段と、前記第4のハッシュ値算定手段により算定された第4のハッシュ値および前記証明内容に含まれる第1のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、を備えたことを特徴とする。

【0021】この請求項6に記載の発明によれば、証明書に含まれる第2のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第3のハッシュ値を算定し、この復号化された第2のハッシュ値および算定された第3のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第4のハッシュ値を算定し、算定した第4のハッシュ値および証明内容に含まれる第1のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる。

【0022】また、請求項7に記載の発明にかかる正当性検証システムは、請求項6に記載の発明において、前記第4のハッシュ値算定手段は、前記読出手段により読み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することを特徴とする。

【0023】この請求項7に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる。

【0024】また、請求項8に記載の発明にかかる正当性検証方法は、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証方法において、前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行工程と、前記証明書発行工程により発行された証明書に基づいて、前記複写データの正当性を検証する検証工程と、を含んだことを特徴とする。

【0025】この請求項8に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【0026】また、請求項9に記載の発明にかかる正当性検証方法は、請求項8に記載の発明において、前記証

明書発行工程は、前記記憶部に記憶した前記原本データについての第1のハッシュ値を算定する第1のハッシュ値算定工程と、前記第1のハッシュ値算定工程により算定された第1のハッシュ値を所定の秘密鍵で暗号化する暗号化工程と、前記暗号化工程により暗号化された暗号データを証明書として出力する証明書出力工程と、を含んだことを特徴とする。

【0027】この請求項9に記載の発明によれば、記憶部に記憶した原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる。

【0028】また、請求項10に記載の発明にかかる正当性検証方法は、請求項8に記載の発明において、前記証明書発行工程は、前記原本データについての第1のハッシュ値を算定する第1のハッシュ値算定工程と、前記第1のハッシュ値算定工程により算定された第1のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成工程と、前記証明内容作成工程により作成された証明内容についての第2のハッシュ値を算定する第2のハッシュ値算定工程と、前記第2のハッシュ値算定工程により算定された第2のハッシュ値並びに前記証明内容作成工程により作成された証明内容からなる証明書を出力する証明書出力工程と、を含んだことを特徴とする。

【0029】この請求項10に記載の発明によれば、原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第2のハッシュ値を算定し、算定した第2のハッシュ値並びに証明内容からなる証明書を出力することとしたので、2重にハッシュ化した高い正当性を保証することができる証明書を発行することができる。

【0030】また、請求項11に記載の発明にかかる正当性検証方法は、請求項10に記載の発明において、前記第1のハッシュ値算定工程は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することを特徴とする。

【0031】この請求項11に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる。

【0032】また、請求項12に記載の発明にかかる正当性検証方法は、請求項9に記載の発明において、前記検証工程は、前記証明書発行工程により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、前記所定の記憶部に記憶した原本データのハッシュ値を

算定するハッシュ値算定工程と、前記算定工程により算定されたハッシュ値および前記復号化工程により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、を含んだことを特徴とする。

【0033】この請求項12に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる。

【0034】また、請求項13に記載の発明にかかる正当性検証方法は、請求項10に記載の発明において、前記検証工程は、前記証明書に含まれる前記第2のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、前記証明書に含まれる証明内容についての第3のハッシュ値を算定する第3のハッシュ値算定工程と、前記復号化工程により復号化された第2のハッシュ値および前記第3のハッシュ値算定工程により算定された第3のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出工程と、前記読出工程により読み出された原本データについての第4のハッシュ値を算定する第4のハッシュ値算定工程と、前記第4のハッシュ値算定工程により算定された第4のハッシュ値および前記証明内容に含まれる第1のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、を含んだことを特徴とする。

【0035】この請求項13に記載の発明によれば、証明書に含まれる第2のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第3のハッシュ値を算定し、この復号化された第2のハッシュ値および算定された第3のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第4のハッシュ値を算定し、算定した第4のハッシュ値および証明内容に含まれる第1のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる。

【0036】また、請求項14に記載の発明にかかる正当性検証方法は、請求項13に記載の発明において、前記第4のハッシュ値算定工程は、前記読出工程により読み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することの特徴とする。

【0037】この請求項14に記載の発明によれば、読

み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる。

【0038】また、請求項15に記載の発明にかかる記録媒体は、前記請求項8～14のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項8～14の動作をコンピュータによって実現することができる。

【0039】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0040】図1は、本実施の形態で用いる正当性検証システムのシステム構成を示すブロック図である。同図に示す正当性検証システムは、原本の保存データを保持する原本性保証電子保存装置100と、この原本の保存データのコピーを原本性保証電子保存装置100から受け取る外部装置110とをネットワークで接続したものである。

【0041】すなわち、この正当性検証システムでは、原本性保証電子保存装置100が大容量記憶媒体101上に保持する原本のコピーを作成する際に、このコピーが原本と同一であることを検証できる保存証明書を発行し、これにより外部装置110上でコピーの正当性を検証できるようにしている。

【0042】同図に示すように、原本性保証電子保存装置100は、大容量記憶媒体101と、通信ポート102と、プログラム格納媒体103と、内部記憶媒体104と、内部タイマ105と、証明書発行部106と、制御部107とからなる。

【0043】大容量記憶媒体101は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやCD-Rなどからなる。通信ポート102は、ネットワークを介して外部装置110との通信をおこなうためのインターフェース部であり、たとえばLANカードなどの通信モデムなどからなる。

【0044】プログラム格納媒体103は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なEEPROMや読み出し専用のROMなどからなる。

【0045】内部記憶媒体104は、各種プログラムの実行に必要なパラメータを記憶するEEPROMなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。内部タイマ105は、制御部107

の本体をなすプロセッサ 106 がプログラムの実行時に所得する時刻を計時するタイマである。

【0046】証明書発行部 106 は、原本性保証電子保存装置 100 が大容量記憶媒体 101 上に保持する原本のコピーを作成した場合に、外部装置 110 からの要求に基づいてこのコピーが原本と同一であることを検証できる保存証明書を発行する処理部である。

【0047】具体的には、原本の保存データは、データ属性ファイル、データアクセス履歴ファイル、データ認証ファイルおよびコンテンツファイルにより形成されるが、このうち外部装置にコピーを作成する対象となるのは、基本的に最新バージョンの状態（属性情報含む）だけであり、アクセス履歴についてまで外部にコピーを作成する必要はないので、この証明書発行部 106 は、コンテンツファイルのうちの最新バージョンに相当するファイルと、データ属性情報のみを対象として保存証明書を作成する。

【0048】なお、大容量記憶媒体 101 については、図中に破線で示したように原本性保証電子保存装置 100 から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置 100 と物理的に一体化し、通信ポート 102 以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【0049】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【0050】制御部 107 は、その実体はプロセッサであり、プログラム格納媒体 103 に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行することになる。

【0051】具体的には、この制御部 107 では、大容量記憶媒体 101 上に保持した原本のコピーを作成した場合に、外部装置 110 からの要求に応答して証明書発行部 106 に対して保存証明書の発行を指示し、この証明書発行部 106 により発行された保存証明書を外部装置 110 に送信する。これにより、外部装置 110 は、この保存証明書をを用いて複写データの正当性を検証することができる。

【0052】つぎに、外部装置 110 の構成について説明する。図 1 に示すように、この外部装置 110 は、通信ポート 111 と、記憶部 112 と、検証部 113 と、制御部 114 とからなる。

【0053】通信ポート 111 は、ネットワークを介して原本性保証電子保存 100 との通信をおこなうためのインターフェース部であり、記憶部 112 は、原本性保証電子保存装置 100 からネットワーク通信により受け取った原本の複写データなどを記憶する記憶媒体であ

り、制御部 114 は、外部装置 110 の全体制御をおこなう制御部である。

【0054】検証部 113 は、原本性保証電子保存装置 100 から複写データとともに受け取った保存証明書に基づいて、この複写データの正当性すなわちこの複写データが大容量記憶媒体 101 上に保持した原本の保存データと一致するか否かを検証する処理部である。

【0055】すなわち、この検証部 113 が、保存証明書に基づいて複写データの正当性を効率良く検証するので、この外部装置 110 上に原本を移動しなくとも、この複写データが大容量記憶媒体 101 上に保持した原本の保存データと一致するか否かを確認することができる。

【0056】上記構成を有する原本性保証電子保存装置 100 および外部装置 110 からなる正当性検証システムを用いることにより、原本の保存データを複写した複写データの正当性を外部装置 110 上で効率良く検証することができる。

【0057】つぎに、図 1 に示した証明書発行部 106 による保存証明書の作成手順について説明する。図 2 は、図 1 に示した証明書発行部 106 による保存証明書の作成手順を示すフローチャートであり、また、図 3 は、図 1 に示した証明書発行部 106 による保存証明書の作成概念を説明するための説明図である。

【0058】図 2 および図 3 に示すように、この証明書発行部 106 は、外部装置 110 から保存証明書取得要求とともに、保存証明書の取得対象となる保存データの保存データ識別番号を受け付けたならば、後述する最新バージョン正当性検証処理をおこない（ステップ S201～S202）、正当性の検証に失敗したならば（ステップ S202 否定）、エラー処理（ステップ S211）の後に処理を終了する。

【0059】これに対して、正当性の検証を成功した場合（ステップ S202 肯定）には、データ属性情報ファイル 301 と最新バージョンのコンテンツファイル全体に対してハッシュ値を計算してファイルハッシュ値 308 とする（ステップ S203）。

【0060】図 3 の例においては、保存データ 300 が、データ属性情報ファイル 301 と、データアクセス履歴ファイル 302 と、データ認証ファイル 303 と、バージョン 1 情報 304 と、バージョン 2 情報 305 と、バージョン 3 情報 306 とからなるので、このデータ属性情報ファイル 301 および最新バージョンのコンテンツファイルを合わせたデータ 307 についてハッシュ値を計算して、これをファイルハッシュ値 308 としている。

【0061】そして、このファイルハッシュ値 308、内部タイマ 105 から取得した現在の日時情報（保存証明取得日時情報）、装置復号鍵（装置公開鍵）および保存データ識別番号を合わせて保存証明内容 309 とする

(ステップS204)。

【0062】また、この保存証明内容309に対してハッシュ値を計算し、これを保存証明内容ハッシュ値310とし(ステップS205)、この保存証明内容ハッシュ値310を装置暗号鍵(装置秘密鍵)で暗号化して、これを保存証明内容署名311とする(ステップS206)。そして、先の保存証明内容309に保存証明内容署名を311付与して保存証明書とし(ステップS207)、この保存証明書を外部装置110に送出する(ステップS208)。

【0063】なお、コンテンツ取得フラグが真(TRUE)であり、コンテンツの要求がなされている場合(ステップS209肯定)には、データ属性情報ファイルと最新バージョンのコンテンツファイルとを外部装置に送出した後に(ステップS210)処理を終了する。

【0064】上記一連の処理をおこなうことにより、複写データの正当性を検証するための保存証明書を作成し、該作成した保存証明書を外部装置110に送信することができる。

【0065】つぎに、図1に示した検証部113による保存証明書の検証処理について説明する。図4は、図1に示した検証部113による保存証明書の検証処理手順を示すフローチャートである。

【0066】同図に示すように、まず最初に保存証明書から保存証明内容署名並びに装置公開鍵証明書を取り出して(ステップS401～S402)、この装置公開鍵証明書を検証し(ステップS403)、装置公開鍵証明書の検証に失敗したならば(ステップS404否定)、公開鍵証明書の正当性の確認ができないことをユーザに警告し(ステップS405)、エラー処理をおこなった後に(ステップS415)処理を終了する。

【0067】これに対して、装置公開鍵証明書の検証に成功したならば(ステップS404肯定)、この装置公開鍵で保存証明内容署名を復号し(ステップS406)、保存証明書の保存証明内容部分についてハッシュ値を計算する(ステップS407)。

【0068】そして、計算したハッシュ値と先に復号した保存内容署名とを比較し(ステップS408)、両者が一致しない場合(ステップS408否定)には、保存証明書が壊れていることをユーザに警告し(ステップS409)、エラー処理をおこなった後に(ステップS415)処理を終了する。

【0069】一方、両者が一致する場合(ステップS408肯定)には、保存証明書とともに保存してあるデータ属性情報ファイル、最新バージョンのコンテンツファイルすべてを合わせたもののハッシュ値を計算した後(ステップS410)、保存証明書からファイルハッシュ値を取り出す(ステップS411)。

【0070】そして、計算したハッシュ値がファイルハッシュ値とを比較し(ステップS412)、両者が一致

しない場合(ステップS412否定)には、保存証明書とともに保存してあるファイルが改変されていることをユーザに警告し(ステップS413)、エラー処理をおこなった後に(ステップS415)処理を終了する。

【0071】これに対して、両者が一致する場合(ステップS412肯定)には、保存証明書の確認が成功した旨を保存証明書の日時情報とともにユーザに表示した後に(ステップS414)、処理を終了する。

【0072】上記一連の処理をおこなうことにより、証明書発行部106により発行された保存証明書に基づいて、検証部113が複写データの正当性を検証することができる。

【0073】ところで、上記検証部113がおこなう検証処理では、保存証明書の証明対象となるコンテンツに変更がない場合を示したが、場合によっては、原本性保証電子保存装置100の内部においては、当該コンテンツが最新の状態でない状況も生じ得る。

【0074】そこで、かかる場合には、外部装置110が原本性保証電子保存装置100に対して保存証明書を提示することにより、保存証明書の正当性の検証と、その保存証明書が対象とするコンテンツが最新の状態であるか否かを確認できることとする。なお、かかる検証処理は、原本性保証電子保存装置100の証明書発行部106によりおこなわれることとなる。

【0075】図5は、図1に示した原本性保証電子保存装置100がおこなう保存証明書の正当性の検証処理並びにその保存証明書が対象とするコンテンツが最新の状態であるか否かの確認処理手順を示すフローチャートである。

【0076】同図に示すように、まず最初に、受け取った保存証明書から保存証明内容署名並びに装置公開鍵証明書を取り出し(ステップS501～S502)、この装置公開鍵証明書が内部記憶媒体104に記録されている装置公開鍵証明書と一致するか否かを確認し(ステップS503)、両者が一致しない場合(ステップS503否定)には、エラー処理をおこなった後に(ステップS518)処理を終了する。

【0077】これに対して、両者が一致する場合(ステップS503肯定)には、装置公開鍵で保存証明内容署名を復号し(ステップS504)、保存証明書の保存証明内容部分についてハッシュ値を計算する(ステップS505)。

【0078】そして、計算したハッシュ値と先に復号した保存証明内容署名が一致するか否かを確認し(ステップS506)、両者が一致しない場合(ステップS506否定)には、エラー処理をおこなった後に(ステップS518)処理を終了する。

【0079】これに対して、両者が一致する場合(ステップS506肯定)には、保存証明書から保存データ識別番号を取得し(ステップS507)、この保存データ

識別番号を渡して後述する最新バージョンの正当性検証処理をおこない（ステップS508）、検証に失敗したならば（ステップS509否定）、エラー処理をおこなった後に（ステップS518）処理を終了する。

【0080】これに対して、検証処理に成功したならば（ステップS509肯定）、保存証明書から保存証明書取得日時情報を取得し（ステップS510）、データ属性情報ファイルから最終更新日時情報を取得する（ステップS511）。

【0081】そして、最新更新日時の方が保存証明書取得日時よりも後である場合（ステップS512肯定）には、更新されていることを示すステータスコード、最終更新日時情報を外部装置110に対して送出して（ステップS513）、処理を終了する。

【0082】これに対して、最新更新日時が保存証明書取得日時よりも後ではない場合（ステップS512否定）には、読み出したデータ属性情報ファイル、最新バージョンのコンテンツファイルをすべて合わせたもののハッシュ値を計算し（ステップS514）、保存証明書からファイルハッシュ値を取り出し（ステップS515）、計算したハッシュ値がファイルハッシュ値と一致するか否かを確認する（ステップS516）。

【0083】その結果、両者が一致しない場合（ステップS516否定）には、エラー処理をおこなった後に（ステップS518）処理を終了し、両者が一致する場合（ステップS516肯定）には、最新の状態であることを示すステータスコード、最終更新日時を外部装置110に送出して（ステップS517）、処理を終了する。

【0084】上記一連の処理をおこなうことにより、保存証明書の正当性の検証と、その保存証明書が対象とするコンテンツが最新の状態であるか否かを確認することができる。

【0085】つぎに、図2および図5に示した最新バージョンの正当性検証処理について具体的に説明する。図6は、図2および図5に示した最新バージョンの正当性検証処理手順を示すフローチャートである。

【0086】同図に示すように、まず最初に大容量記憶媒体101から保存データリストファイルを読み出し（ステップS601）、保存データリストファイルに受け取った保存データ識別番号に該当する保存データエントリを取得し（ステップS602）、該当する保存データエントリが存在するか否かを確認する（ステップS603）。

【0087】その結果、該当する保存データエントリが存在しない場合（ステップS603否定）には、エラー処理をおこなった後に（ステップS617）処理を終了し、該当する保存データエントリが存在する場合（ステップS603肯定）には、保存データエントリから保存データMACを取得するとともに（ステップS60

4）、保存データ識別番号に該当する保存データのデータ認証ファイルを大容量記憶媒体101から読み出し（ステップS605）、データ認証ファイルからハッシュリストMACを取り出す（ステップS606）。

【0088】なお、この保存データMACおよびハッシュリストMACのMACとは、メッセージ認証子（Message Authentication Code）のことであり、内部記憶媒体104内に記憶した秘密鍵を用いて作成される。

【0089】そして、このハッシュリストMACと保存データMACが一致するか否かを確認し（ステップS607）、両者が一致しない場合（ステップS607否定）には、エラー処理をおこなった（ステップS617）後に処理を終了し、両者が一致する場合（ステップS607肯定）には、ハッシュリストMACを装置暗号鍵（公開鍵）で復号してハッシュリストハッシュとし（ステップS608）、データ認証ファイルのハッシュリストMAC以外の部分のハッシュ値を計算する（ステップS609）。

【0090】そして、計算したハッシュ値と先のハッシュ値が一致するか否かを確認し（ステップS610）、両者が一致しない場合（ステップS610否定）には、エラー処理をおこなった（ステップS617）後に処理を終了し、両者が一致する場合（ステップS610肯定）には、保存データ識別番号に該当する保存データの最新バージョンに相当するコンテンツファイルをすべて大容量記憶媒体101から読み出し（ステップS611）、読み出したコンテンツファイルについてそれぞれハッシュ値を計算する（ステップS612）。

【0091】そして、計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致するか否かを確認し（ステップS613）、両者が一致しない場合（ステップS613否定）には、エラー処理をおこなった（ステップS617）後に処理を終了し、両者が一致する場合（ステップS613肯定）には、保存データ識別番号に該当する保存データのデータ属性情報ファイルを大容量記憶媒体101から読み出し（ステップS614）、読み出したデータ属性情報ファイルについてハッシュ値を計算する（ステップS615）。

【0092】そして、計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致するか否かを確認し（ステップS616）、一致しない場合（ステップS616否定）には、エラー処理をおこなった後に（ステップS617）処理を終了し、一致する場合（ステップS616肯定）には、そのまま処理を終了する。

【0093】上述してきたように、本実施の形態では、原本性保証電子保存装置106の証明書発行部106が原本をコピーした複写データについての保存証明書を発行し、外部装置110の検証部113が保存証明書に基づいて複写データの正当性を検証するよう構成したので、外部装置110上に原本のコピーを保持する場合

に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【0094】

【発明の効果】以上説明したように、請求項1に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証システムが得られるという効果を奏する。

【0095】また、請求項2に記載の発明によれば、記憶部に記憶した原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる正当性検証システムが得られるという効果を奏する。

【0096】また、請求項3に記載の発明によれば、原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第2のハッシュ値を算定し、算定した第2のハッシュ値並びに証明内容からなる証明書を出力することとしたので、2重にハッシュ化した高い正当性を保証することができる証明書を発行することができる正当性検証システムが得られるという効果を奏する。

【0097】また、請求項4に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる正当性検証システムが得られるという効果を奏する。

【0098】また、請求項5に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる正当性検証システムが得られるという効果を奏する。

【0099】また、請求項6に記載の発明によれば、証明書に含まれる第2のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第3のハッシュ値を算定し、この復号化された第2のハッシュ値および算定された第3のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第4のハッシュ値を算定し、算定した

第4のハッシュ値および証明内容に含まれる第1のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる正当性検証システムが得られるという効果を奏する。

【0100】また、請求項7に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる正当性検証システムが得られるという効果を奏する。

【0101】また、請求項8に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証方法が得られるという効果を奏する。

【0102】また、請求項9に記載の発明によれば、記憶部に記憶した原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる正当性検証方法が得られるという効果を奏する。

【0103】また、請求項10に記載の発明によれば、原本データについての第1のハッシュ値を算定し、算定した第1のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第2のハッシュ値を算定し、算定した第2のハッシュ値並びに証明内容からなる証明書を出力することとしたので、2重にハッシュ化した高い正当性を保証することができる証明書を発行することができる正当性検証方法が得られるという効果を奏する。

【0104】また、請求項11に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第1のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる正当性検証方法が得られるという効果を奏する。

【0105】また、請求項12に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる正当性検証方法が得られるという効果を奏する。

【0106】また、請求項13に記載の発明によれば、証明書に含まれる第2のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第3のハッシュ値を算定し、この復号化された第2のハッシュ値および算定された第3のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第4のハッシュ値を算定し、算定した第4のハッシュ値および証明内容に含まれる第1のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる正当性検証方法が得られるという効果を奏する。

【0107】また、請求項14に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第4のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる正当性検証方法が得られるという効果を奏する。

【0108】また、請求項15に記載の発明にかかる記録媒体は、請求項8～14のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項8～14の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態で用いる正当性検証システムの

システム構成を示すブロック図である。

【図2】図1に示した証明書発行部による保存証明書の作成手順を示すフローチャートである。

【図3】図1に示した証明書発行部による保存証明書の作成概念を説明するための説明図である。

【図4】図1に示した検証部による保存証明書の検証処理手順を示すフローチャートである。

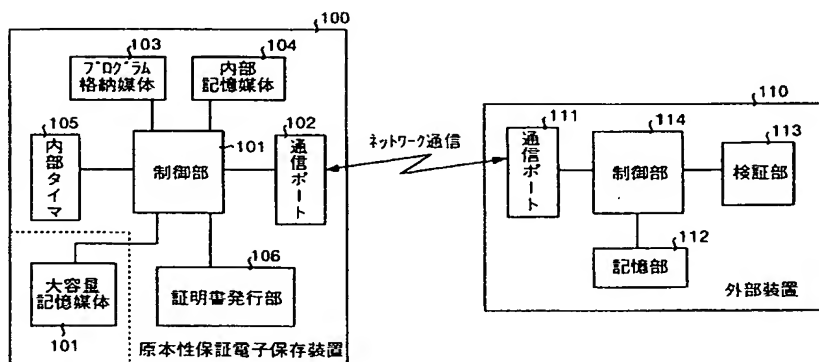
【図5】図1に示した原本性保証電子保存装置がおこなう保存証明書の正当性の検証処理並びにその保存証明書が対象とするコンテンツが最新の状態であるか否かの確認処理手順を示すフローチャートである。

【図6】図2および図5に示した最新バージョンの正当性検証処理手順を示すフローチャートである。

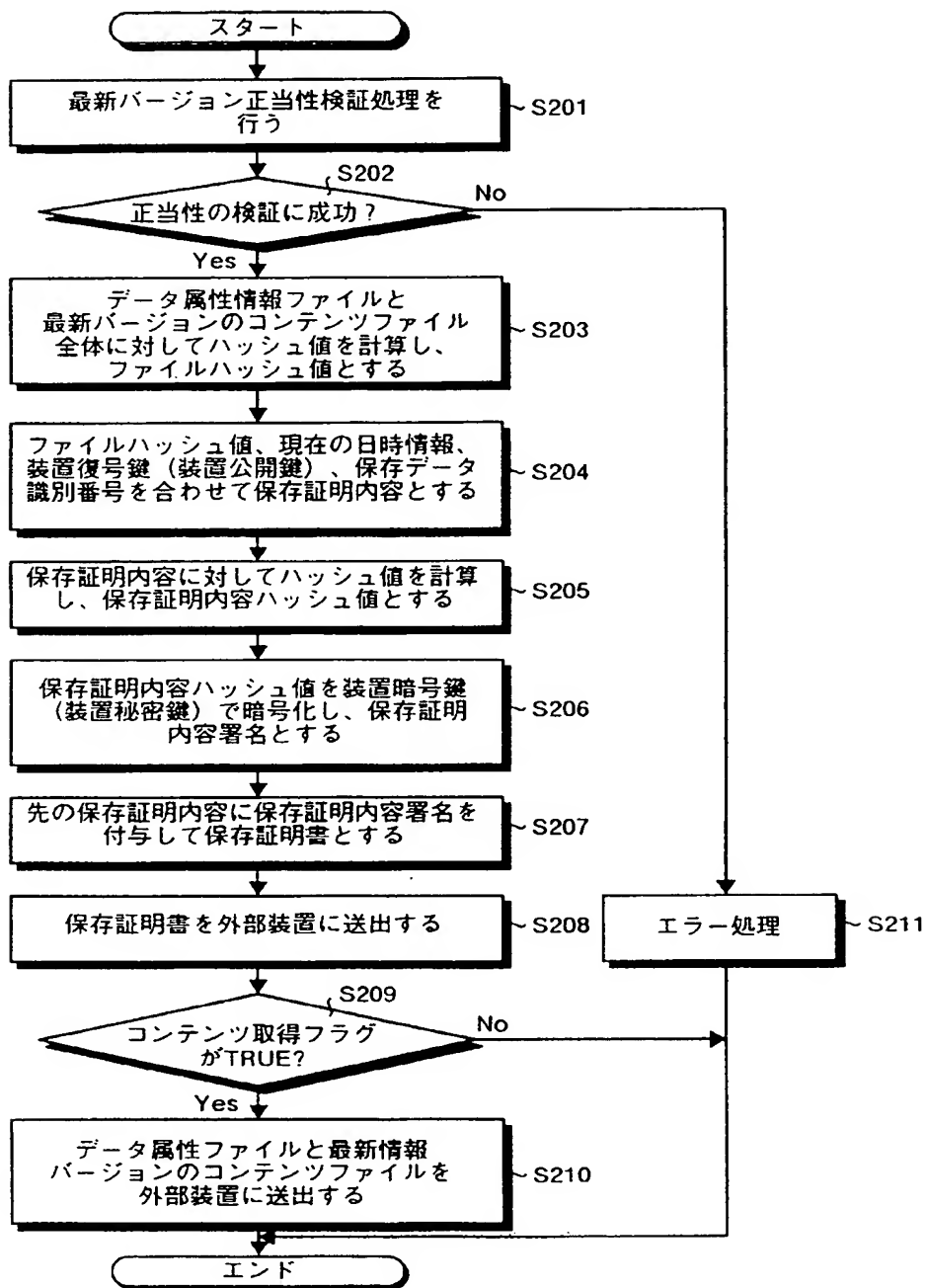
【符号の説明】

- 100 原本性保証電子保存装置
- 101 大容量記憶媒体
- 102 通信ポート
- 103 プログラム格納媒体
- 104 内部記録媒体
- 105 内部タイマ
- 106 証明書発行部
- 107 制御部
- 110 外部装置
- 111 通信ポート
- 112 記憶部
- 113 検証部
- 114 制御部

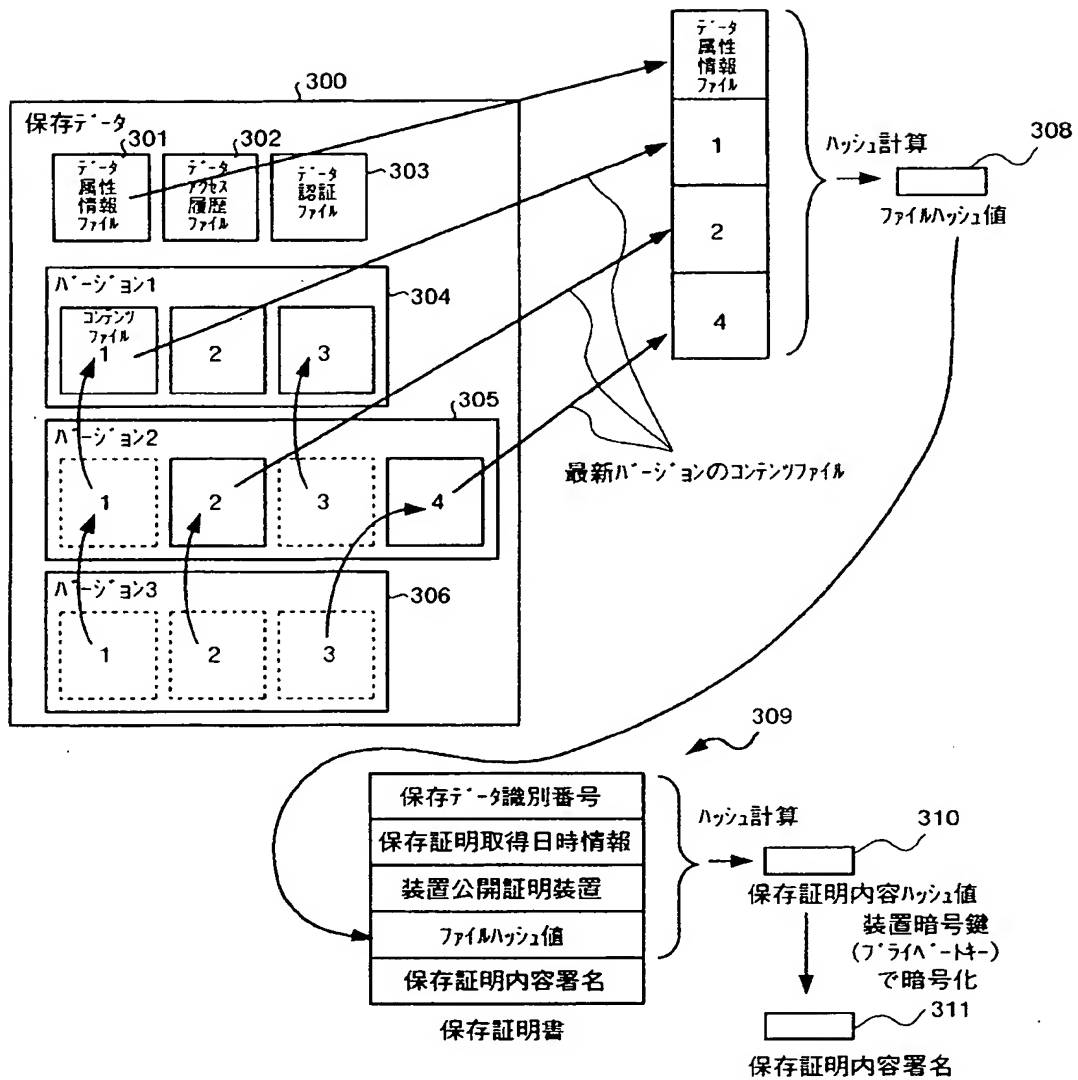
【図1】



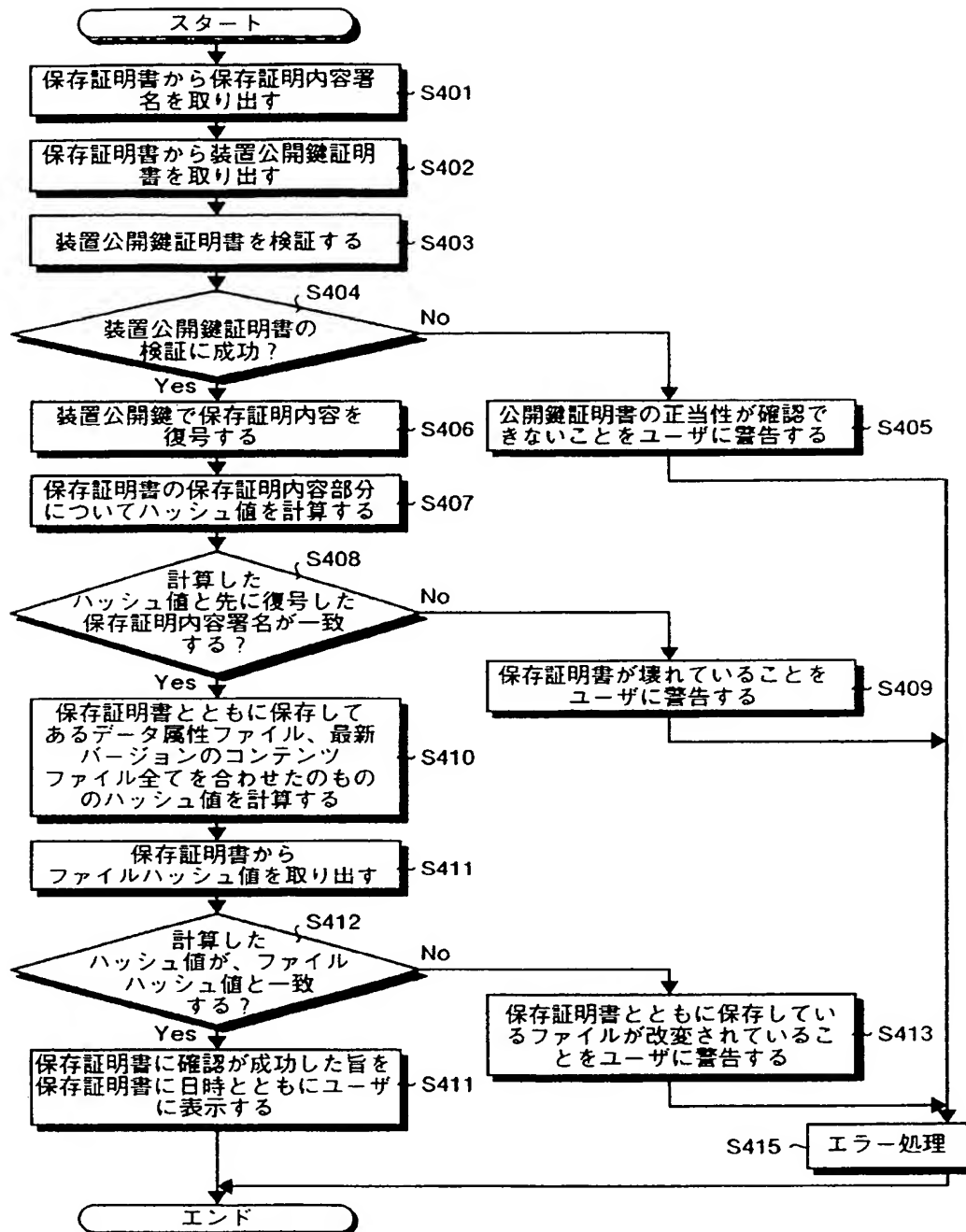
【図2】



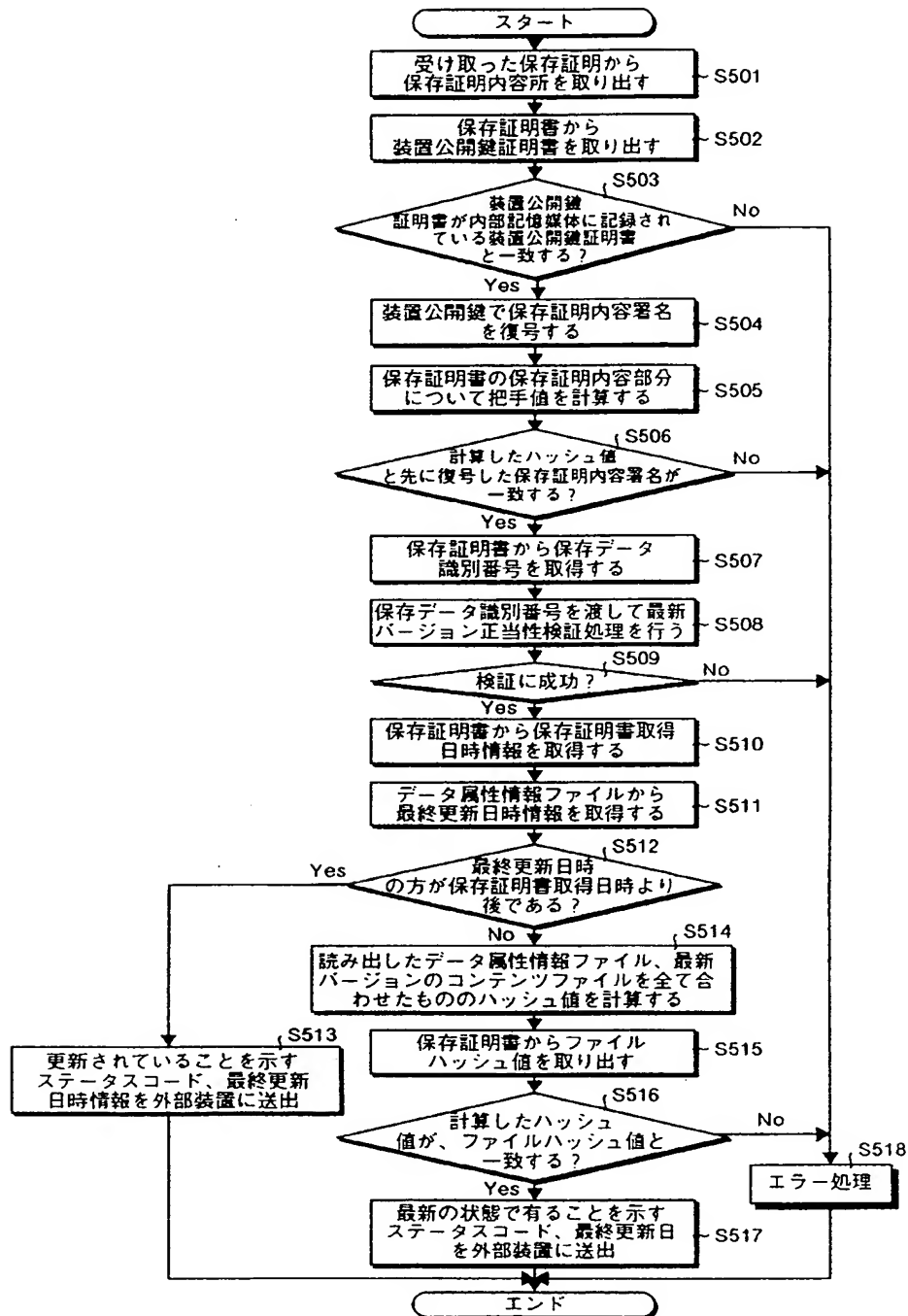
【図3】



【図4】



【図5】



【図6】

